

62807-158
Makio MIZUNO
January 27, 2004

日本国特許庁
JAPAN PATENT OFFICE *McDermott, Will & Emery*

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年 4月22日

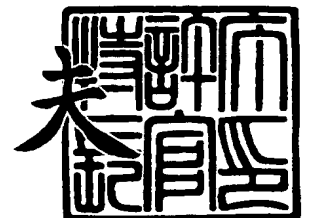
出願番号
Application Number: 特願2003-116451
[ST. 10/C]: [JP 2003-116451]

出願人
Applicant(s): 株式会社日立製作所

2004年 1月 8日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-3109676

【書類名】 特許願

【整理番号】 H03001701A

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/16 645

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

 【氏名】 水野 真喜夫

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社 日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

 【電話番号】 03-3212-1111

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 ブロックデータをキャッシュするキャッシュストレージ装置及び該装置を備えたネットワークストレージシステム

【特許請求の範囲】

【請求項 1】

ネットワークに接続されたキャッシュストレージ装置であって、
前記ネットワークにはさらに、記憶媒体上の論理アドレスとデータ長を指定するブロックデータを送受信する1つ以上のクライアント及び1つ以上の記憶装置が接続され、前記クライアントと前記記憶装置の間で送受信する前記データを一時的に蓄積することを特徴とするキャッシュストレージ装置。

【請求項 2】

前記クライアントから前記キャッシュストレージ装置に対してライト要求が発行された場合、前記ライト要求が示す前記キャッシュストレージ装置内の領域をロックすることを特徴とする請求項 1 記載のキャッシュストレージ装置。

【請求項 3】

前記クライアントから前記キャッシュストレージ装置に対してライト要求が発行された場合、前記ライト要求が示す前記キャッシュストレージ装置内の領域をロックするとともに前記キャッシュストレージ装置内の領域に対応する前記記憶装置内の領域もロックすることを特徴とする請求項 1 記載のキャッシュストレージ装置。

【請求項 4】

前記ロックをするかしないかを、前記キャッシュストレージ装置内のロック状況を示すロック管理テーブルをもとに判断することを特徴とする請求項 2 または 3 に記載のキャッシュストレージ装置。

【請求項 5】

前記ロック管理テーブルは、少なくとも前記キャッシュストレージ装置内の領域を判別するインデックス、前記キャッシュストレージ装置内の領域の前記ロックの状況を示すフラグ、前記キャッシュストレージ装置内の領域に対応する前記記憶装置内の領域の前記ロックの状況を示すフラグで構成することを特徴とする請

求項 4 記載のキャッシュストレージ装置。

【請求項 6】

前記クライアントから受信した前記ロックの要求に対する許可を前記クライアントへ発行したあと、前記許可に対する応答確認が無かった場合、前記ロックの要求を無効とすることを特徴とする請求項 2 または 3 に記載のキャッシュストレージ装置。

【請求項 7】

前記キャッシュストレージ装置内の領域に対する処理の要求が前記クライアントから無い場合に、前記キャッシュストレージ装置内の領域に対応する前記記憶装置内の領域に対して前記キャッシュストレージ装置内の領域の内容のライト要求を発行することを特徴とする請求項 2 または 3 に記載のキャッシュストレージ装置。

【請求項 8】

前記キャッシュストレージ装置内の領域と前記記憶装置内の領域との対応を示すアドレス対応テーブルを備える請求項 7 記載のキャッシュストレージ装置。

【請求項 9】

前記記憶装置へデータを送信するときに、該データに対して暗号化を施すことを特徴とする請求項 7 記載のキャッシュストレージ装置。

【請求項 10】

前記クライアントから一定時間要求が無かった場合、前記ロックしている前記記憶装置内の領域の解放要求を前記記憶装置に対して発行することを特徴とする請求項 2 または 3 に記載のキャッシュストレージ装置。

【請求項 11】

前記クライアントの認証を行って、通信を許可した時点で、前記クライアントに対してアクセスを許可する前記キャッシュストレージ装置内の領域をロックすることを特徴とする請求項 1 記載のキャッシュストレージ装置。

【請求項 12】

前記クライアントの認証を行って、通信を許可した時点で、前記クライアントに対してアクセスを許可する前記キャッシュストレージ装置内の領域をロックする

とともに前記キャッシュストレージ装置内の領域に対応する前記記憶装置内の領域もロックすることを特徴とする請求項1記載のキャッシュストレージ装置。

【請求項13】

前記キャッシュストレージ装置内の領域に対する処理が前記クライアントから無い場合に、前記キャッシュストレージ装置内の領域に対応する前記記憶装置内の領域に対して前記キャッシュストレージ装置内の領域の内容のライト要求を発行することを特徴とする請求項11または12に記載のキャッシュストレージ装置。

【請求項14】

前記記憶装置へデータを送信するときに、該データに対して暗号化を施すことを特徴とする請求項13記載のキャッシュストレージ装置

【請求項15】

請求項1において、前記クライアントからのリード要求を受けた場合前記キャッシュストレージ装置上に該当するデータが存在する場合そのデータを前記クライアントに送信し、存在しない場合は前記記憶装置に該当する前記データを要求し、前記記憶装置から送られてきた前記データを前記クライアントに送信することを特徴とするキャッシュストレージ装置。

【請求項16】

前記クライアント、前記記憶装置の識別情報を管理する識別情報管理手段が前記ネットワークに接続されているネットワークストレージシステムにおいて、前記識別情報管理手段に登録されている前記記憶装置の識別情報を変更する手段を備えることを特徴とする請求項1記載のキャッシュストレージ装置

【請求項17】

記憶媒体上の論理アドレスとデータ長を指定するブロックデータを送受信する1つ以上のクライアント及び1つ以上の記憶装置、並びに前記記憶装置の識別情報を管理する識別情報管理手段がネットワークに接続されており、さらに前記クライアントと前記キャッシュストレージ装置との間に前記クライアントの処理を代行する代行処理装置が接続されているネットワークストレージシステムであって、前記代行処理装置が該キャッシュストレージ装置の前記識別情報を前記識別情

報管理手段から取得し、前記代行処理装置がその識別情報を元に該キャッシュストレージ装置に対する処理を前記クライアントに代わり実行し、その処理結果を前記クライアントに送信することを特徴とするネットワークストレージシステム。

【請求項 18】

記憶媒体上の論理アドレスとデータ長を指定するブロックデータを送受信する1つ以上のクライアント、及び1つ以上の記憶装置、並びにキャッシュストレージ装置を備え、さらに前記クライアント、前記記憶装置、前記キャッシュストレージ装置とを接続する結合装置を備え、

前期結合装置が、前記クライアントから前記記憶装置への要求を一旦前記キャッシュストレージ装置へ送信し、

前記キャッシュストレージ装置がその要求を処理し、その処理結果を前記クライアントへ送信した後で、

前記キャッシュストレージ装置から記憶装置へ前記要求を発行することを特徴とするネットワークストレージシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、記憶装置の論理アドレスとデータ長を指定するブロックデータを一時的に蓄積するストレージシステムにおいてレスポンス性能の改善、さらに障害発生時のオーバヘッドを削減する技術に関する。

【0002】

【従来の技術】

ストレージの接続形態は、サーバ直結型のDirect Attached Storage(DAS)からネットワーク接続型のStorage Area Network(SAN)が主流となっている。

SANを実現する伝送方式としてファイバチャネルを用いたSAN(FC-SAN)が一般的である。

ファイバチャネルは伝送媒体として光を使うため信頼性が非常に高くプロトコルとしてもオーバヘッドが少ないため、実効転送性能は非常に高い。

ここで、転送性能で遅れを取っていたイーサネット（登録商標）が、ネットワークの技術の進歩に伴い高速化され、接続距離無制限、低コスト、相互接続性を売りにSANへ適用されつつある。

これはFC-SANと区別するためにIP-SANと呼ぶ。

IP-SANを実現する手段としていくつか候補があるが、iSCSI(internet SCSI)が最も有力と言われている。

信頼性が低いイーサネット（登録商標）をインフラとして使うiSCSIでは、データ転送の信頼性を確保するためにTCP/IPを用いる。

しかし、この場合信頼性を確保する反面転送に係るオーバーヘッドが大きくなるという問題がある。

そのため、規格上の転送性能ではファイバチャネルを越えつつあるが実効転送性能で見ると転送オーバーヘッドの影響で劣ってしまう。

それは、転送に係わる処理は装置内のプロセッサによるソフトウェア処理で行われていたことに原因がある。

この問題を解決する手段として、ソフトウェア処理されていた部分を専用のハードウェアで処理することでカバーするアプローチがある。

TCP/IP offload engine(TOE)と呼ばれ、処理全体をオフロードする方式、データ移動のみをオフロードする方式、ハードウェア内のプロセッサコアに処理させることで装置内のプロセッサからオフロードする方式がある。

一方で、TCPはコネクション型でこの層を介して送られて来るデータの順序保証、誤り訂正、障害発生時の再送処理を行う。特に障害発生時の再送処理のオーバーヘッドはサーバとストレージ間の接続距離に比例し大きくなり性能に悪影響を及ぼす。

尚、ファイバチャネルは先に述べたとおり信頼性が確保されているため基本的に再送処理は行わないため再送処理に伴うオーバーヘッドはない。

このTCPにおける再送処理の問題を解決する手段として、サーバとストレージの間にキャッシュデバイスを配置し、サーバからの要求をそのデバイスでキャッシングする。再送処理が発生した場合は、サーバからではなくキャッシュデバイスから再送することにより上記オーバーヘッドを削減する効果が期待できる。

さらに、本来ストレージで処理されるアクセスがその中間に存在するキャッシュデバイスで処理されるため転送遅延が軽減され性能向上の効果が期待できる。

Webアクセスにおいては、「Webキャッシュ」としてサーバから取得したページを一旦ローカルにキャッシュするのが一般的である。

再度表示する必要がある場合、毎回そのサーバからページを取得するのではなくローカルにキャッシュしたページを表示することでレスポンス性能を向上させる。

サーバ側ではページを絶えず更新していることを考慮すると、ローカルにキャッシングしたページとサーバで管理するページとで鮮度を保証する必要がある。

これは、キャッシングしたページの内容が、既にサーバ側で更新されていた内容を反映していない場合、「WEBキャッシュ」としての効力を失うことになるためである。

Webアクセスを実現するためのプロトコルHTTP(HyperText Transport Protocol)では鮮度を保証する手段として、要求に対するレスポンスヘッダに定義されているAge、ボディヘッダにExpires、Last-Modifiedなどのパラメータ、及び現在時刻からローカルのキャッシュを使用可能かどうか判定する。Ageはサーバがレスポンスを送信してからのクライアントの推定経過時間を示しその経過時間が有効期限を過ぎていなければ新鮮と判断する。Expiresはレスポンスが新鮮でなくなる時点での日付、時間を示す。Last-Modifiedはサーバが最後に更新した日付、時刻を示す。ただし、キャッシュ可能な命令はリード(サーバからの読み込み)系のものに限定されている。

ファイルシステムにおけるリードデータのキャッシュ方法に関しては、特許文献1、特許文献2に開示された「広域分散ファイルシステム」、「データ配信方法及びデータ配信プログラムを格納した記憶媒体」等がある。

前者の技術は、ファイルサーバが接続されたネットワークに、クライアントがキャッシュサーバを介して接続されたシステムにおいて、アクセス頻度の高いファイルをキャッシュサーバ上に先読みしておくことで高速なファイルアクセスを実現する技術が開示されている。本技術はリードデータのキャッシュのみを想定しており、ライトデータの書き込み時に発生するデータの整合性の問題を想定して

いないため、本発明のファイルサーバに対するアクセス制御（ロック）は行っていない。

後者の技術は、データサーバとキャッシュサーバとクライアントがネットワークを介して接続されたシステムにおいて、データ要求をしたクライアントへのデータ配信の負荷が小さく、通信時間の遅延が小さいキャッシュサーバのみを介してデータを配信することで、無駄なデータが他のキャッシュサーバに蓄積されることを防ぐ技術が開示されている。本公知例もリードデータのキャッシュのみを想定しているため、本発明のファイルサーバに対するアクセス制御（ロック）は行っていない。

【特許文献 1】

特開平 1 1 - 2 4 9 8 1 公報

【特許文献 2】

特開 2 0 0 1 - 2 9 0 7 8 7 公報

【0 0 0 3】

【発明が解決しようとする課題】

Web キャッシュ技術、特許文献 1、特許文献 2 に開示された技術はファイルデータを対象としており、かつリードデータのみをキャッシングする。ファイルデータとはファイルシステムがアクセス可能な単位データである。

トランザクション性能が要求されるアプリケーションにはブロックレベルでのアクセスが望ましい。ファイルデータへのアクセスは最終的にブロックレベルでのアクセスになるためその分のオーバーヘッドがトランザクション性能に影響を与えるためである。たとえばデータベースアプリケーションではリードアクセスだけではなくライトアクセスも行われる。

ライトアクセスで問題になるのは、そのキャッシングされたデータに対して複数のクライアントがアクセスする場合である。

複数のクライアントから同一領域にライトアクセスのリクエストが発行された場合、キャッシュデバイスでその双方のリクエストが競合し、双方がデータの書き込み又は書き換えをしようとするためデータの保証が出来ない。

別の問題として、信頼性の低い（例えばイーサネット（登録商標））伝送路を使

う場合伝送障害がしばしば発生しアプリケーションに対するレスポンス性能が低下する。レスポンス性能が低下するとトランザクション性能も低下する。

通常、ネットワーク上で障害が発生すると送信元と受信先との間で再送処理を開始する。

再送処理のトリガーは基本的に送信元のタイムアウト検出であり、その間通信がストップする。

さらに、再送処理に加えて送信元と受信先間の接続距離に比例した伝送遅延も加わるため転送効率が低下する。

この結果、アプリケーションに対するレスポンス性能が低下してしまう。

別の問題として、送信元、受信元の間ではデータ通信経路が通信プロトコルによって決められているあるアルゴリズムにしたがって決定されるため、必ずしもキャッシュデバイスを通過しないということである。

iSCSIの下位プロトコルTCP/IPは、経路制御プロトコルがあるポリシーに従って最適な経路を検索する。代表的な経路制御プロトコルとしてRIP、OSPFがある。

一例としてRIPに関して図15を使って説明する。

クライアント1505からサーバ1560へは3通りの通信経路があるとする。

1510、1515、1520、1525、1530、1535、1540、1550はルータでありネットワーク間を結合する装置である。

各ルータ間で1つのネットワークを構成しており、それぞれが独立したネットワークである。

例えば、1510-1515間のネットワークと1510-1520間のネットワークは独立した異なるネットワークである。

図15では、クライアント1505、サーバ1560間において、ルータ1515、ルータ1520-1525、ルータ1530-1535-1540を経由する3通りの経路が存在する。

RIPでは、ホップ(hops)を使って最適経路を決定する。

ホップは、クライアント1505からサーバ1560の間で通過するネットワークの数のことであり、例えば3つのネットワークを通過するとそれは3ホップと表す。

RIPは、このホップ数が一番少ない経路が最短経路と判断する。

図15では、1515を経由する経路は1ホップ、1520を経由する経路は2ホップ、1530

を經由する経路は3ホップとなりRIPに従ってクライアント1505、サーバ1560間は通信経路1565が最適な経路となる。

ここで、キャッシュデバイスがルータ1510、1520との間に存在すると経路制御プロトコルにより最適な経路1565が選択されているためキャッシュデバイスを通過しない。

つまり、クライアント1505からのデータはキャッシュされずにそのままサーバに到達してしまい上記の問題は解決されない。

OSPFなどの経路選択プロトコルでも判定基準は異なるものの最小コストの経路を選択するため、仮にキャッシュデバイスが最小コストの経路上に存在しない場合、キャッシュの恩恵を必ずしも受けることが出来ない。

本発明の主たる目的は、記憶媒体上のアドレスとデータ長を指定するブロックデータをクライアントとストレージ間のキャッシュストレージで一旦キャッシングし、再送処理はクライアントからではなくキャッシュストレージとの間で行うことで転送効率を上げることにある。

本発明のさらに別の目的は、クライアントとキャッシュストレージ間でロックアクセス制御を行うことで、クライアントが複数存在する場合にリクエストの競合を防止することにある。

本発明のさらに別の目的は、ネームサービスに登録されているストレージの情報をキャッシュストレージの情報に置き換えることで、ネットワーク上のキャッシュストレージにクライアントが通信できるようにすることにある。ネームサービスとは、あるネットワーク上のネットワーク機器の識別情報を管理するサービスを指す。

本発明のさらに別の目的は、セキュリティを確保するためにキャッシュストレージとストレージ間は暗号化通信を行うことにある。キャッシュストレージとストレージ間が一般の公衆網など信頼できない伝送路を介する場合特にセキュリティ確保が重要となる。

【0 0 0 4】

【課題を解決するための手段】

上記問題を解決するために、クライアントとストレージの間にネットワークに

接続可能でブロックデータを一時的に蓄積するキャッシュストレージを設ける。

【0 0 0 5】

【発明の実施の形態】

[実施例 1]

以下、本発明に係わるキャッシュストレージ装置の実施例 1 を図面に示しさらに詳細に説明する。

図1は、本発明のキャッシュストレージ装置を含むネットワークストレージシステムの全体構成を示している。

105、106はクライアントであり、ストレージターゲットに対してリクエストを発行する。ストレージターゲットとは本来クライアントと通信するストレージを指す。

110、115はネームサービスであり、TCP/IPネットワークにおいてはDNS(Domain Name System)、iSCSIにおいてはiSNS(Internet Storage Name Service)サーバ、SLP DA(Service Location Protocol-Directory Agent)などを指す。

これらは、独立したネットワーク毎に存在する。

図1では、2つのネットワークが存在し各ネットワークに1つのネームサービスが存在する。

通常、耐障害性を高める目的でネームサービスは冗長構成にするが図1では省略する。

DNSは、各デバイスに与えられるホスト名から対応するIPアドレスを取得するシステムであり、DNSサーバがその対応をデータベースで管理する。

インターネットではあるページにアクセスする場合、IPアドレスを指定するのではなくURL（例えばwww.abcd.comのように）を指定するのが一般的である。

それは、数字の羅列であるIPアドレスは憶えにくく、そのページが一体どのような内容かというのが一目で判断できないためである。

【0 0 0 6】

図1で、例えばクライアント105のホスト名がabc、IPアドレスが192.168.0.1、クライアント106のホスト名がdef、IPアドレスが192.168.0.10とする。

クライアント105がクライアント106と通信する場合、クライアント106のホスト

名を元にネームサービス110にクライアント106のIPアドレスを問い合わせる。
ネームサービス110が管理しているデータベースからクライアント106のホスト名
に対応するIPアドレスをクライアント105へ返す。

ネームサービス110から受け取ったIPアドレスで初めてクライアント106との通信
が可能となる。

iSNSは、IPネットワーク上のiSCSIストレージデバイスとファイバチャネルスト
レージデバイスの管理フレームワークであり、iSNSサーバがネットワーク上のク
ライアント、ストレージデバイスを管理する。

デバイスの識別には、iSCSIストレージデバイスの場合iSCSIネーム、ファイバチ
ャネルデバイスの場合WWPN(World Wide Pote Name)を使う。

【 0 0 0 7 】

図16でiSNSにおけるデバイス検出を簡単に説明する。

クライアント1605、iSCSIストレージデバイス1615、iSNSサーバ1610がネットワ
ーク1620を介して接続した図である。

ここで、iSCSIストレージデバイス1615は既に接続されiSNSサーバ1610上にiSCSI
ストレージデバイス1615の情報が登録されているものとする。

クライアント1605をネットワーク1620に接続すると、まず自分自身の情報をiSNS
サーバ1610へ登録する。

これにより、ネットワーク1620に存在するiSCSIストレージデバイス1615にクラ
イアント1605が同一ネットワーク上に存在するという通知がiSNSサーバから送ら
れる。

そして、クライアント1605は、iSCSIストレージデバイスを検出するクエリーをi
SNSサーバ1610へ送信しiSCSIストレージデバイス1615の情報（iSCSIネーム、IP
アドレス、ポート番号）を取得する。

以上を経て、iSCSIストレージデバイス1615へ通信可能となる。

図 1 の説明にもどると、120はネットワークであり、クライアント105、106、ネ
ームサービス110を接続する手段で例えばLAN(Local Area Network)などである。
125はキャッシュストレージであり、クライアントとは別のネットワークに接続
され、クライアント105、106が記憶装置130と行う通信においてクライアント105

から送られるデータを一時蓄積する。

130は記憶装置であり、ディスクドライブ等のストレージデバイスを有する装置である。

135はネットワークであり、キャッシュストレージ125、記憶装置130、ネームサービス115が接続されている。

ここで、ネットワーク120をネットワーク1、ネットワーク135をネットワーク2と区別しそれぞれ独立した異なるネットワークと定義する。

140はネットワーク結合装置で、異なるネットワークを接続するための手段として用いる。

【0 0 0 8】

図2は、本発明に係わるキャッシュストレージの実施例1における全体構成図を示している。

キャッシュストレージは、ディスク制御装置205とディスク駆動装置235で構成する。

205はディスク制御装置で、ネットワークとディスク駆動装置235とのインターフェースを持つ。

ディスク制御装置205は、チャンネル制御部、キャッシュメモリ制御部、共有メモリ制御部、ディスク制御部で構成する。

206は入出力バスであり、ネットワーク2と接続され、このネットワーク2とディスク制御装置205内チャンネル制御部210とを接続するバスである。

210はチャンネル制御部であり、ネットワークインタフェースを持ち、クライアントとのユーザデータ送受信、ディスク制御装置205内部の制御情報などの共有データへのアクセスを制御する。

チャンネル制御部210は、ディスク制御装置205内に複数存在する。

215は、キャッシュメモリ制御部であり、クライアント、及びディスク駆動装置にあるユーザデータを一時的に格納するキャッシュメモリを備え、チャンネル制御部、またはディスク制御部からのキャッシュメモリアクセスを制御する。

220は共有メモリ制御部であり、ディスク制御装置205内部での通信に関する制御情報を格納する共有メモリを備え、チャンネル制御部210、及びディスク制御部230

からの共有メモリアクセスを制御する。

共有メモリ制御部220には、キャッシュストレージ内のデバイスのロック状況を示すロック管理テーブル225、アドレス対応テーブル226を備える。

225はロック管理テーブルで、どのデバイスがロックされているかを示す。

226はアドレス対応テーブルで、キャッシュストレージ内のデバイスとそれに対応する記憶装置内デバイスとの対応付けをする。

クライアントからのユーザデータの一時蓄積場所であるキャッシュメモリ、もしくはディスク駆動装置235に存在するデータを記憶装置へ格納するときに指定する記憶装置のアドレスとキャッシュストレージ内デバイスのアドレスとを対応付けて管理する。

230はディスク制御部であり、ディスク駆動装置235との通信制御、及びキャッシュメモリ・共有メモリへのアクセスなどを行う。

ディスク制御部235は、ディスク制御装置205内に複数存在する。

チャネル制御部210とキャッシュメモリ制御部215、及び共有メモリ制御部220との間の接続や、ディスク制御部230とキャッシュメモリ制御部215、及び共有メモリ制御部220との間の接続はバス接続、またはスター接続などの形態をとるが、本発明では特に定めない。

235は、ディスク駆動装置であり、複数のドライブ240で構成しユーザデータなどを格納する。

ディスク駆動装置235のドライブ240に対して1つ以上のiSCSIネームを割り当てる。iSCSIネームとはiSCSIプロトコルを認識する個々の機器を識別するための情報である。

【0009】

図3は、本発明の実施例1におけるチャネル制御部210の構成ブロックを示している。

305はプロトコル制御部であり、ネットワークパケットを受信する。受信したパケットがiSCSIパケットの場合さらにその中からiSCSIヘッダ、SCSIコマンド、データなどを取り出しチャネル制御プロセッサ310へ渡す。iSCSIパケット以外のパケットは適切な処理（例えばICMPリクエストであればICMPリプライを発行）をす

る。

また、SCSIコマンドの処理結果をチャネル制御プロセッサ310から受け取りiSCSIパケットを生成する。

iSCSIパケットをネットワークパケットにカプセル化し入出力パス206を通じてネットワーク2へ送出する。

310はチャネル制御プロセッサであり、プロトコル制御部305からのSCSIコマンド、データなどの受信、解析を行い、解析したリクエストの内容に従い、ディスク制御装置内部に指示を与えるプロセッサである。

320はデータ転送制御部であり、チャネル制御プロセッサ305からの指示により、クライアントのユーザデータ転送、及びディスク駆動装置にあるデータを読み出す。

325は共有データ制御部であり、制御情報等の共有データが格納されている共有メモリへのアクセスを制御する。図17はネットワークパケット、iSCSIパケットの関係の一例を示している。1701はネットワークパケットでEtherパケット、IPパケット、TCPパケット、TCPデータグラムで構成する。1705はEtherパケットでありデータリンク層に関連する制御情報（MACアドレス等）とデータを含む。1710はIPヘッダでEtherパケット1705のデータ部分に相当しIP層に関連する制御情報（IPアドレス等）とデータを含む。1715はTCPパケットでIPパケット1710のデータ部分に相当しTCP層に関連する制御情報（ポート番号、シーケンス番号等）を含むTCPヘッダ1725、iSCSIパケット1730を含む。iSCSIパケット1730はiSCSIに必要な制御情報とSCSIコマンド、データを含む。

【0 0 1 0】

図4は本発明の実施例1におけるロック管理テーブル400を示している。

405はiSCSIネームで、キャッシュストレージ内のデバイスを識別するiSCSIネームを示す。

410はロックステータスで、iSCSIネーム405に対応するキャッシュストレージ内のデバイス、及び記憶装置内のデバイスのロック状況を示す。

420はキャッシュロックフラグで、“OFF”はiSCSIネーム405に対応するキャッシュストレージ内のデバイスがロックされていない状態、“ON”はロックされている状

態を示す。

425は記憶装置ロックフラグで、“OFF”はiSCSIネーム405で表されるキャッシュストレージ内デバイスに対応する記憶装置内のデバイスがロックされていない状態、“ON”はロックされている状態を示す。

このテーブルを上記のように利用することでキャッシュストレージ、及び記憶装置のロック状況を把握することが可能となりアクセスが競合してもデータを保証できる。

図13は、本発明の実施例1におけるアドレス対応テーブル1300を示している。

1305はデバイス名であり、キャッシュストレージ内のストレージデバイスに割り当てられたiSCSIネームを示す。

1310は記憶装置アドレスであり、デバイス名1305に対応する記憶装置内のストレージデバイスのiSCSIネームである。

キャッシュストレージのデータを記憶装置へ格納するときにまず記憶装置内のストレージデバイスに対しログインする。

そのログインするデバイスのiSCSIネームを指定するときにアドレス対応テーブルを参照しログインパラメータとして記憶装置アドレスを使う。このテーブルを上記のように利用することで記憶装置に対するログインに必要な情報を容易に参照することが出来る。

【 0 0 1 1 】

図5は、実施例1におけるクライアント毎に記憶装置のデバイスが割り当てられている時のクライアントとキャッシュストレージとの通信フローとキャッシュストレージと記憶装置との通信フローを示している。

ここでの通信はライト処理とする。

図5では、クライアント毎にあらかじめデバイスを割り当てているためキャッシュストレージでリクエストが競合しない。

従って、デバイスをロックする処理が不要となる。

まず、クライアントから割り当てられたキャッシュストレージ内のデバイスに対してログインを発行する（ステップ505）。

この時に、本来記憶装置に到達するログインをキャッシュストレージへと導く必

必要がある。

そのため最初のログインするデバイスの情報を取得するときに、ネームサービスが記憶装置ではなくキャッシュストレージの情報を送信することで解決する。キャッシュストレージの情報とは、例えばIPアドレス、ポート番号、iSCSIネームである。

これはキャッシュストレージとネームサービスとの間であらかじめ通信して決める。

それは、TCPのデータで通信する方法や、iSNSのVender Specific Messageでお互いに取り決めたメッセージを通信してクライアントからの情報取得要求のときに記憶装置の情報ではなくキャッシュストレージの情報をクライアントに見せる。ログインを受け取ったキャッシュストレージはログインを許可するステータスと共にログイン応答メッセージをクライアントに送信する（ステップ510）。

この時点で、クライアントとキャッシュストレージ内のデバイスとのセッションを確立した状態となる。

クライアントはリクエストを発行する（ステップ515）。

キャッシュストレージはそのリクエストを処理しステータスを含むメッセージをクライアントに送信する（ステップ520）。ステータスとは、そのリクエスト処理が正常終了したかどうか、異常終了した場合その要因を示す。

必要に応じてステップ515、520の処理を繰り返し最後のリクエストを発行した（ステップ525）後のキャッシュストレージからのメッセージを受ける（ステップ530）とクライアント側の処理は終了する（ステップ535）。

クライアントとの通信を終えた後、記憶装置へのデータ格納処理に入る。

記憶装置へのデータ格納処理に入るタイミングは本発明の実施には影響しないので、ここでは特に定めない。

クライアントとの通信終了直後でも、適当なタイミングに行っても構わない。

データ格納処理に入るとキャッシュストレージから記憶装置へデータ転送を指示するリクエストを発行する（ステップ540）。

記憶装置はそのリクエストに従い所定の領域に格納する（ステップ545）。

リクエストに対する応答をキャッシュストレージへ送信し処理を終了する（ステ

ップ550)。

ここで、クライアントからリード要求を受けた場合、もしその要求されたデータがキャッシュストレージに存在する場合、そのデータをクライアントへ送信し、なければ記憶装置からデータを読み出しクライアントへ送信する。

記憶装置からデータを読み出した場合、クライアントに送信すると共にキャッシュストレージ上にそのデータを残し次回同一要求を受けた場合にそのキャッシュしたデータを使用してもよい。

以上の処理により、従来記憶装置まで通信するところをクライアントにより近い場所での通信ですむため、クライアントから見ると応答時間が短縮されレスポンス性能、トランザクション性能の改善につながる。

【0012】

図14に本発明の実施例1における伝送路障害が発生した場合の転送フローを示している。

なお、図14では図5のステップ540以降の処理を示す。

ステップ540では、キャッシュストレージに格納されたデータを記憶装置へ格納する処理を指示するリクエストを発行する。

ここで、伝送路で障害が発生したとする(1405)。

キャッシュストレージは要求したリクエストに対する応答を受信できる状態になっている。

ところが、送ったリクエストが記憶装置へ到達する前に障害が発生したため記憶装置はこのリクエストを処理できない。よって記憶装置はリクエストに対する応答が出来ない。

キャッシュストレージは応答が無いためタイムアウトを検出し再送処理を開始する。

このような動作により、従来であればクライアントまで影響が及ぶ再送処理(1415)が記憶装置に近い位置にあるキャッシュストレージまでで抑える(1410)ことが出来るため再送処理の負荷軽減につながる。

クライアントから見ると、トランザクション性能の改善につながる。

信頼性の低いネットワークであればより効果が大きくなる。

実施例1によれば、記憶媒体の論理アドレスとデータ長を指定するブロックデータ通信において、クライアントと記憶装置間の距離が非常に離れている場合にその間にキャッシュストレージを設置し、クライアントからのブロックデータをキャッシングすることによりレスポンス性能を改善させると共に再送処理の軽減によるトランザクション性能も改善させることが出来る。

[実施例 2]

以下、本発明に係わるキャッシュストレージ装置の実施例2を図6から図9に示しさらに詳細に説明する。

以下特に説明のない部分は実施例 1 と同じとする。

図6に本発明の実施例2におけるクライアント、キャッシュストレージ、記憶装置間の通信フローを示している。

通信はライト処理とする。

ここで、実施例1と異なるのはクライアントがキャッシュストレージのデバイスをロック制御している点である。

つまり、クライアントからのリクエストがキャッシュストレージで競合する場合である。

実施例2においては、ロック制御をReserve、ReleaseというSCSIコマンドで実現する。

Reserveコマンドは領域全体を特定のデバイスのために予約して排他的に占有できるようにするコマンドである。

ReleaseコマンドはReserveコマンドで排他的に占有している領域全体を解放するコマンドである。

Reserve、Releaseコマンドの詳細は、CQ出版社「SCSI-2詳細解説」で述べられている。

なお、実施例2では実施例1で示したログイン処理は既に完了済みとし省略する。キャッシュストレージ、記憶装置のロック管理テーブルはそれぞれ図7-1、図8-1の状態とする。

クライアントがキャッシュストレージに対してリクエストを発行する前に該デバイスのロック要求を発行する。



これにはReserveコマンドを用いる（ステップ605）。

キャッシュストレージはReserveコマンドを受けるとキャッシュストレージ上の該領域のロック状態を確認する。

キャッシュストレージは該領域がロックされていなければロックしステータス"Good"をクライアントへ送信する。

既にロックされていればステータス"Reservation conflict"をキャッシュストレージがクライアントへ送信する。

このとき、クライアントがロック要求を発行したクライアントの状況を確認するためにロックOKを示すコマンドを発行してもよい（ステップ610）。

ステップ610を受けたクライアントはその確認応答のためにロックAcknowledgeをキャッシュストレージに送信する。

これは、他のクライアントからロック要求を受けたときにデッドロックを生じさせないための手段として用いられる。

そして、キャッシュストレージは該領域に対応するロック管理テーブルを更新（図7-2）する（ステップ620）。

クライアントはキャッシュストレージに対してリクエストを発行する（ステップ630）。

キャッシュストレージはそのリクエストを処理しステータスを含む応答をクライアントへ送信する（ステップ640）。

この間、他のクライアントから同一領域に対するロック要求(ステップ645)、もしくはリクエストを受けて（ステップ650）もキャッシュストレージは"Reservation conflict"ステータスを該クライアントに送信しそれら要求を拒絶する。

必要に応じてステップ630、640を繰り返し一連の処理が終了するとクライアントはキャッシュストレージに対してロック解除要求を発行する（ステップ655）。

このときReleaseコマンドを使う。

キャッシュストレージは該領域を開放し、ステータス"Good"をクライアントへ送信する。

このとき、Reserve時と同様にロック解除要求を発行したクライアントの状況を確認するためにロック解除OKを示すコマンドを発行してもよい（ステップ660）

。

ステップ610を受けたクライアントはその確認応答のために解除Acknowledgeをキャッシュストレージに送信する（ステップ665）。

そして、キャッシュストレージは該領域に対応するロック管理テーブルを更新（図7-3）する（ステップ657）。

この後、記憶装置へ該データを送信するために記憶装置と接続している入出力バスを制御するチャンネル制御プロセッサへ処理を引き継ぐ（ステップ670）。

ただし、クライアントとの通信をするチャンネル制御プロセッサがそのまま処理を続行してもよい。

その場合、ステップ670は省略出来る。

記憶装置と通信を開始するためキャッシュストレージはまず記憶装置に対して該領域のロック要求を発行する（ステップ672）。

このときReserveコマンドを使用し指定する領域はアドレス対応テーブルを参照し決定する。

記憶装置はReserveコマンドを受けると記憶装置上の該領域のロック状態を確認する。

記憶装置は該領域がロックされていなければロックしステータス”Good”をクライアントへ送信する。

記憶装置は既にロックされていればステータス”Reservation conflict”をクライアントへ送信する。

このとき、ロック要求を発行した記憶装置の状況を確認するためにロックOKを示すコマンドを発行してもよい（ステップ676）。

ステップ676を受けたクライアントはその確認応答のためにロックAcknowledgeをキャッシュストレージに送信する（ステップ678）。

これは、他のキャッシュストレージ、クライアントからロック要求を受けたときにデッドロックを生じさせないための手段として用いられる。

そして、キャッシュストレージは該領域に対応するロック管理テーブルを更新（図7-4、図8-2）する（ステップ674）。

キャッシュストレージは記憶装置に対してリクエストを発行する（ステップ680

）。

記憶装置はそのリクエストを処理しステータスを含む応答をキャッシュストレージへ送信する（ステップ682）。

必要に応じてステップ680、682の処理を繰り返し、一連の処理が終了するとキャッシュストレージは該領域のロック解除要求を発行する（ステップ684）。

このときReleaseコマンドを使う。

記憶装置は該領域を開放し、ステータス”Good”をキャッシュストレージへ送信する。

このとき、Reserve時と同様にロック解除要求を発行したキャッシュストレージの状況を確認するためにロック解除OKを示すコマンドを発行してもよい（ステップ686）。

ステップ610を受けたクライアントはその確認応答のために解除Acknowledgeをキャッシュストレージに送信する（ステップ688）。

そして、キャッシュストレージは該領域に対応するロック管理テーブルを更新（図7-5、図8-3）する（ステップ690）。

【0013】

図9は、実施例2におけるクライアントが記憶装置を直接ロックする場合の例を示している。

クライアントが記憶装置の領域をロックするためにまずキャッシュストレージに対してロック要求を発行する（ステップ905）。

次にキャッシュストレージが記憶装置に対してロック要求を発行する（ステップ910）。

このとき、Reserveコマンドを使用し該領域の情報はアドレス対応テーブルを参照し決定する。

記憶装置がReserveコマンドを受けると記憶装置上の該領域のロック状態を確認する。

記憶装置は該領域がロックされていなければロックしステータス”Good”をクライアントへ送信する。

既にロックされていれば記憶装置はステータス”Reservation conflict”をクライ

アントへ送信する。

このとき、ロック要求を発行したクライアントの状況を確認するためにロックOKを示すコマンドをキャッシュストレージ経由で発行してもよい（ステップ920、930）。

ステップ930を受けたクライアントはその確認応答のためにロックAcknowledgeをキャッシュストレージ経由で記憶装置へ送信する（ステップ935、940）。

これは、他のクライアント、キャッシュストレージからロック要求を受けたときにデッドロックを生じさせないための手段として用いられる。

そして、記憶装置は該領域に対応するロック管理テーブルを更新（図8-2）する（ステップ925）。

クライアントはキャッシュストレージに対してリクエストを発行する（ステップ945）。

キャッシュストレージはそのリクエストを処理しステータスを含む応答をクライアントへ送信する（ステップ950）。

必要に応じてステップ945、950の処理を繰り返し、一連の処理が終了するとキャッシュストレージは記憶装置へそのデータを送信する処理を開始するが、そのタイミングはクライアントからの一連の処理終了直後など任意のタイミングで行ってよい。

キャッシュストレージはクライアントから受信したデータを記憶装置へ送信するためのリクエストを発行する（ステップ955）。

記憶装置でそのリクエストを処理しステータスをキャッシュストレージへ送信する（ステップ960）。

必要に応じてステップ955、960を繰り返し、一連の処理が終了するとキャッシュストレージがクライアントに対して終了を報告する（ステップ962）。

この報告は、iSCSIのAshynchronous Messageなどを用いる。

ステップ962を受けてクライアントからロック解除要求をキャッシュストレージ経由で記憶装置へ送信する（ステップ965、970）。

記憶装置で該領域を解放し、ステータスをキャッシュストレージ経由でクライアントへ送信する（ステップ972、974）。

このとき、Reserve時と同様にロック解除要求を発行したクライアントの状況を確認するためにロック解除OKを示すコマンドを発行してもよい（ステップ972、974）。

ステップ974を受けたクライアントはその確認応答のために解除Acknowledgeをキャッシュストレージに送信する（ステップ976、978）。

そして、記憶装置は該領域に対応するロック管理テーブルを更新（図7-5、図8-3）する（ステップ980）。

実施例2によれば、キャッシュストレージ、またはキャッシュストレージと記憶装置を他からのアクセスを拒否（ロック）することによって複数のクライアントからリクエストを受けてもデータの更新順序を保証する事が出来る。

なお、実施例1、2においてキャッシュストレージがネットワーク1上に存在しても同じである。

[実施例3]

以下、本発明に係わるキャッシュストレージ装置の実施例3を図示しさらに詳細に説明する。

以下特に説明のない部分は実施例1、2と同じとする。

図10は、実施例3におけるキャッシュストレージ装置を含むネットワークストレージシステムの全体構成を示している。

実施例1、2と異なるのはネットワーク間を接続するネットワーク結合装置がアクセス代理装置に変わっている点である。

1005、1010はクライアントであり、ストレージターゲットに対してリクエストを発行する。

1020、1045はネームサービスであり、TCP/IPネットワークにおいてはDNS(Domain Name System)、iSCSIにおいてはiSNS (Internet Storage Name Service)サーバ、SLP DA(Service Location Protocol-Directory Agent)などを指す。

これらは、独立したネットワーク毎に存在する。

1030はネットワークであり、クライアント1005、1010、ネームサービス1020を接続する手段で例えばLAN(Local Area Network)などである。

1040はキャッシュストレージであり、クライアントとは別のネットワークに接続

しクライアント1005、1010と記憶装置1050との通信においてクライアント1005、1010から送られるデータを一時蓄積する。

1050は記憶装置であり、ディスクドライブ等のストレージデバイスを有する装置である。

1055はネットワークであり、キャッシュストレージ1040、記憶装置1050、ネームサービス1045で構成される。

ここで、ネットワーク1030をネットワーク1、ネットワーク1055をネットワーク2と区別しそれぞれ独立した異なるネットワークと定義する。

1060はアクセス代理装置で、クライアントからのリクエストを代理で行う。

具体的には、クライアントからのリクエストをアクセス代理装置が受け取り、そのリクエストに従いキャッシュストレージと通信を開始する。

通信終了後、ステータス等をアクセス代理装置が受け取りクライアントへ送信する。

実施例1、2におけるクライアントがアクセス代理装置と置き変わったのを除けば同じとなる。

実施例3によれば、クライアントが属するネットワーク（ネットワーク1）と記憶装置が属するネットワーク（ネットワーク2）をアクセス代理装置が中継することでネットワーク1へ不正なデータ流入を防止しつつ、キャッシュストレージによるレスポンス性能向上、トランザクション性能が向上する。

[実施例4]

以下、本発明に係わるキャッシュストレージ装置の実施例4を図示しさらに詳細に説明する。

以下特に説明のない部分は実施例1、2と同じとする。

図11は、実施例4におけるクライアント、キャッシュストレージ、記憶装置間の通信フローを示している。

実施例1、2と異なるのはクライアントがキャッシュストレージのデバイスにログインするときに領域をロックするという点である。

ログイン要求1105をクライアントから受けると、キャッシュストレージ内のロック管理テーブルのキャッシュロックフラグを確認する。

キャッシュストレージはキャッシュロックフラグがOFFの場合はロック要求を受諾、ONの場合は拒否応答をクライアントへ送信する（ステップ1110）。

ロック要求受諾を受けたクライアントはキャッシュストレージへリクエストを発行する（ステップ1130）。

キャッシュストレージはリクエストを処理しそのステータスをクライアントへ送信する（ステップ1135）。

その間他のクライアントからログイン要求（ステップ1120）、リクエスト（ステップ1125）を受けても拒絶する。

必要に応じてステップ1130、1135の処理を繰り返し処理が終了するとキャッシュストレージも該領域のロックを解除する（ステップ1140）。

この後、キャッシュストレージは記憶装置へ該データを送信するために記憶装置と接続している入出力パスを制御するチャネル制御プロセッサへ処理を引き継ぐ（ステップ1145）。

ただし、クライアントとの通信をするチャネル制御プロセッサがそのまま処理を続行してもよい。

その場合、ステップ1145は省略出来る。

キャッシュストレージと記憶装置との通信もクライアントとキャッシュストレージとの通信と同様の流れとなる。

実施例4によれば、ログイン認証時に一括して処理を行うことが出来るためネットワーク上へ送出するパケット量を抑止することが出来る。

[実施例5]

以下、本発明に係わるキャッシュストレージ装置の実施例5を図示しさらに詳細に説明する。

以下特に説明のない部分は実施例1、2と同じとする。

図12は、実施例5におけるキャッシュストレージを含むネットワークストレージシステムの全体構成を示している。

ここで説明のためネットワーク1とネットワーク2をまとめてネットワーク1210で表す。

ネットワークを1つで表すことによって実施例5に影響は与えない。

実施例1、2と異なるのはチャンネル制御部210のキー1205である。

このキー1205はキャッシュストレージ1220、記憶装置1230間の通信を暗号化するためのキーである。

キーは、共有秘密鍵方式、公開鍵方式などあるが本発明では特に定めない。

暗号化通信は図6のステップ672からステップ688まで、図9のステップ950以降からステップ962まで

で行う。

実施例5によれば、記憶装置に格納するデータのセキュリティを確保する通信を行うことが可能となる。

【 0 0 1 4 】

【発明の効果】

SCSIのReserve、Releaseコマンドを使い、かつクライアント、キャッシュストレージによるロック状況を示すロック管理テーブル、およびキャッシュストレージ、記憶装置間のアドレスの対応を示すアドレス対応テーブルを用いることによって、ブロックデータのキャッシングによるレスポンス性能、トランザクション性能の向上、およびクライアント間のデータの一貫性、新鮮さ、セキュリティを保証したデータ通信を行うことが可能となる。

【図面の簡単な説明】

【図 1】

本発明の実施例1におけるネットワークストレージシステムの全体構成を示す。

【図 2】

本発明の実施例1における記憶装置の構成を示す。

【図 3】

本発明の実施例1におけるチャンネル制御部の構成を示す。

【図 4】

本発明の実施例1におけるロック管理テーブルを示す。

【図 5】

本発明の実施例1におけるロックが必要ない場合のクライアントから記憶装置

間の通信フローを示す。

【図 6】

本発明の実施例2におけるロックを使う場合のクライアントから記憶装置間の通信フローを示す。

【図 7】

本発明の実施例2におけるキャッシュストレージのロック管理テーブルの変化を示す。

【図 8】

本発明の実施例2における記憶装置のロック管理テーブルの変化を示す。

【図 9】

本発明の実施例2における同時にキャッシュストレージ、記憶装置をロックした場合のクライアントから記憶装置間の通信フローを示す。

【図 10】

本発明の実施例3におけるネットワークストレージシステムの全体構成を示す。

【図 11】

本発明の実施例4におけるクライアントから記憶装置間の通信フローを示す。

【図 12】

本発明の実施例5におけるクライアントから記憶装置間の通信フローを示す。

【図 13】

本発明の実施例1におけるアドレス対応テーブルを示す。

【図 14】

本発明の実施例1における伝送路で障害が発生した場合を示す。

【図 15】

RIPの説明図を示す。

【図 16】

iSNSにおけるディスカバリを示す。

【図 17】

ネットワークパケットとiSCSIパケットの関係を示す。

【符号の説明】

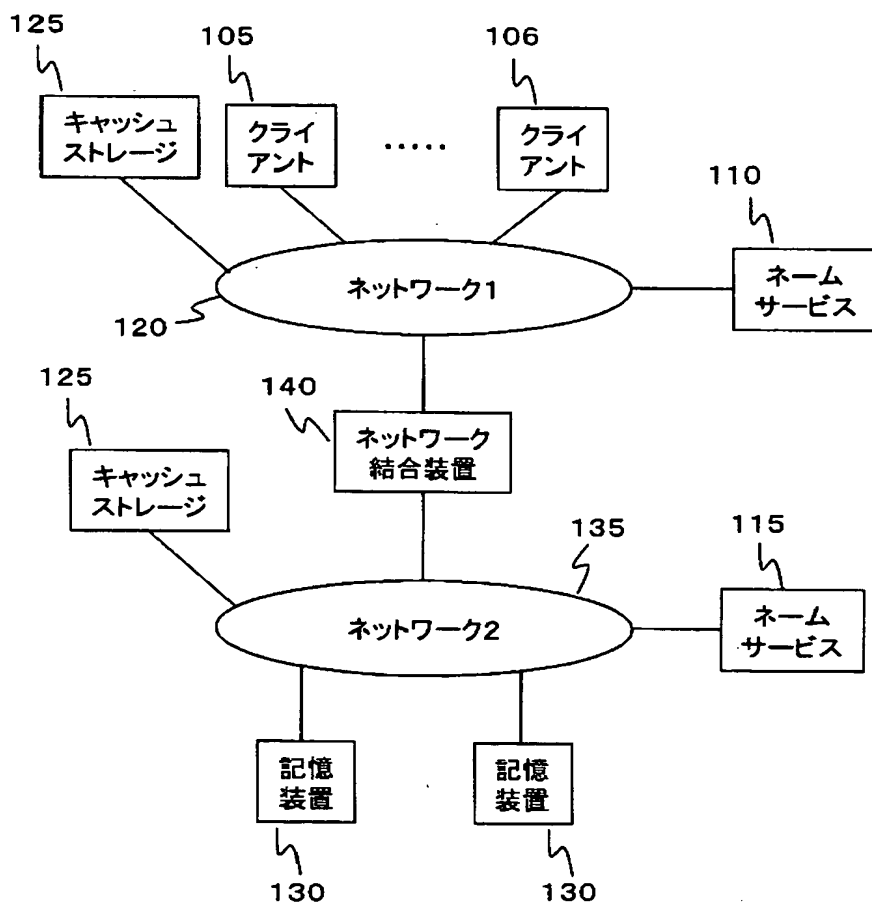
2 0 6：入出力パス
2 1 0：チャンネル制御部
2 1 5：チャンネル制御部
2 2 0：共有メモリ制御部
2 2 5：ロック管理テーブル
2 2 6：アドレス対応テーブル
2 3 0：ディスク制御部
2 3 5：ディスク制御装置
2 4 0：ディスクドライブ。

【書類名】

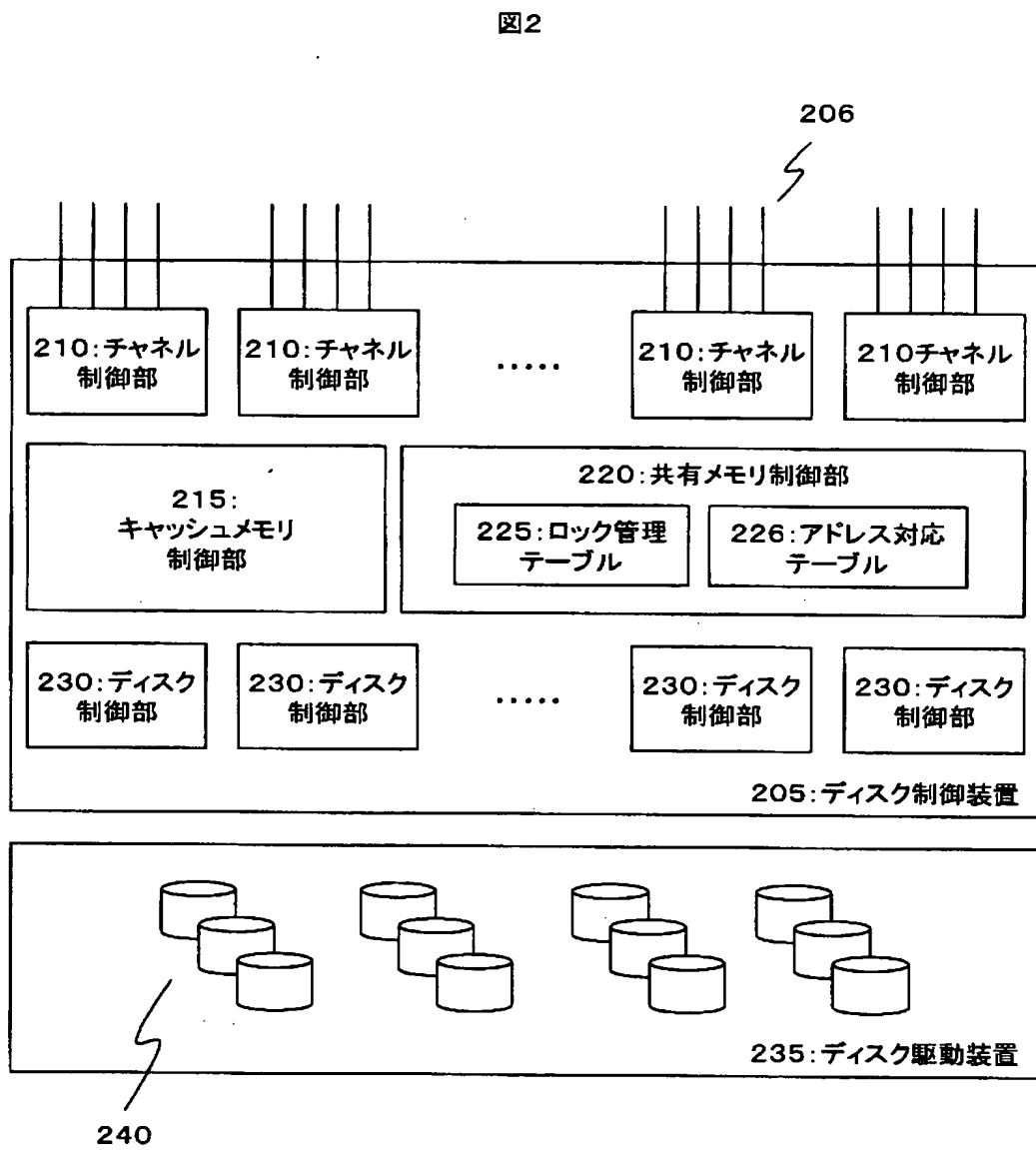
図面

【図 1】

図1

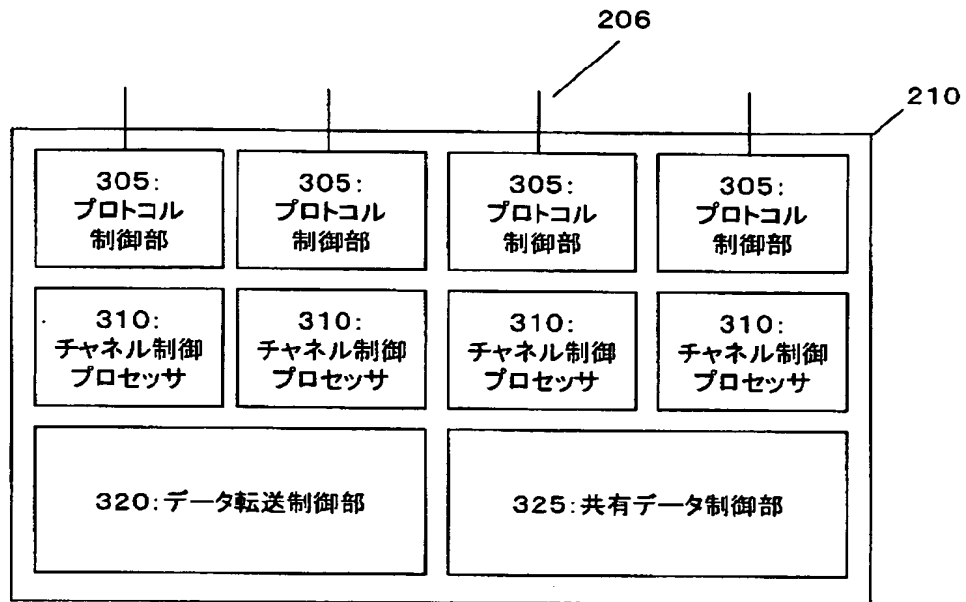


【図 2】



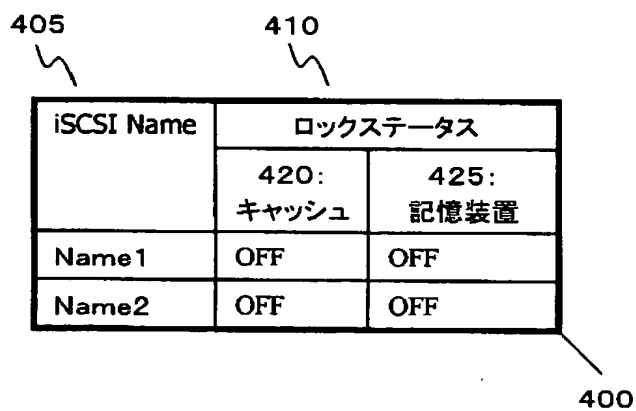
【図 3】

図3



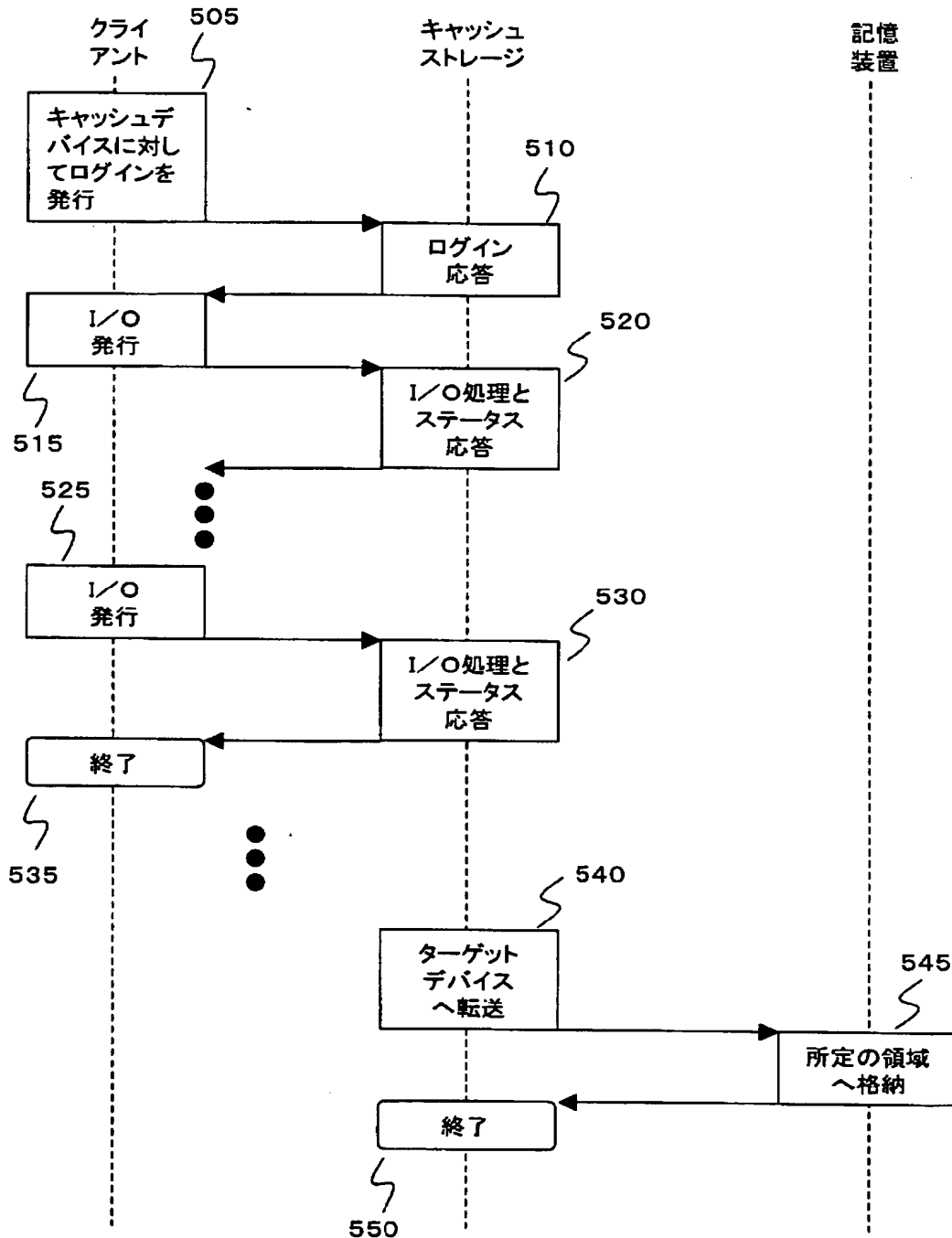
【図 4】

図4



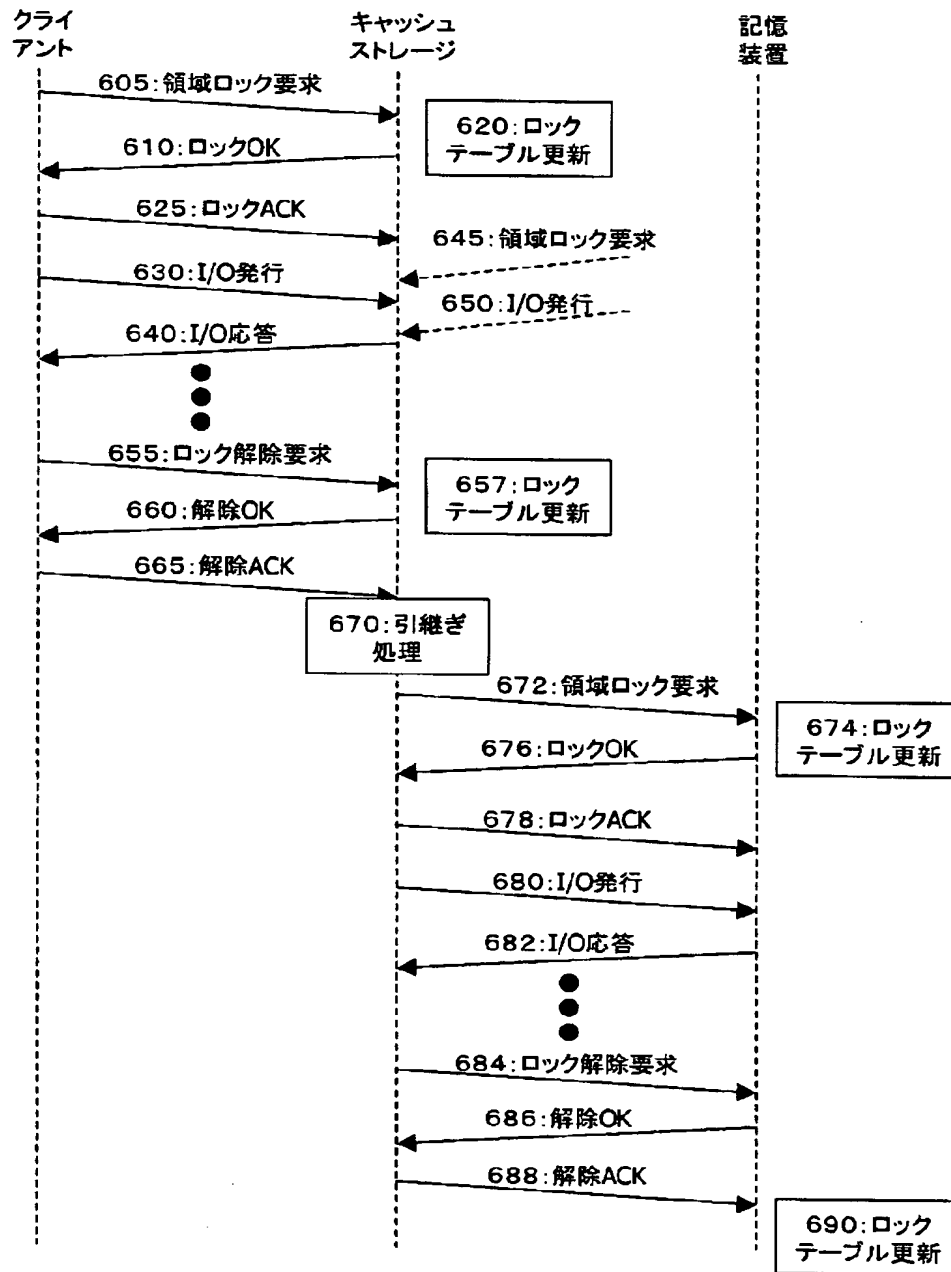
【図 5】

図5



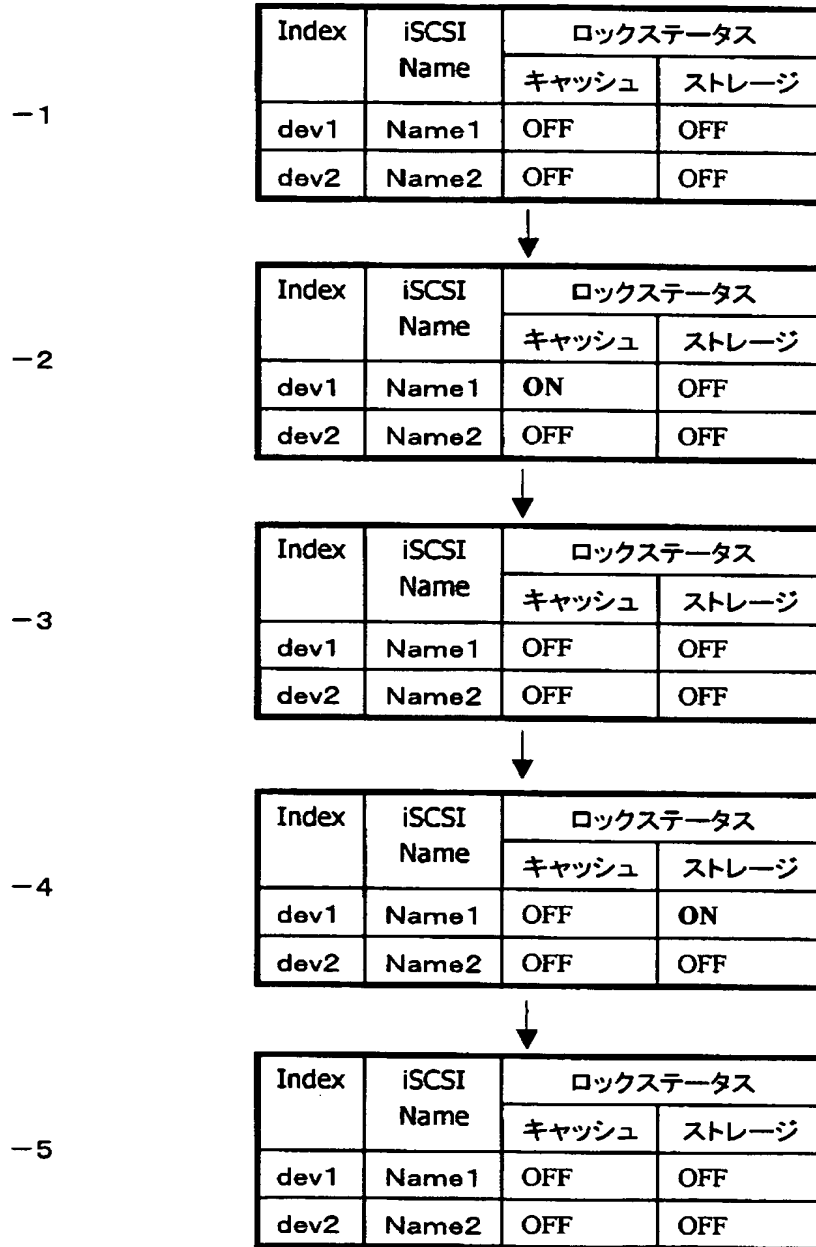
【図 6】

図6



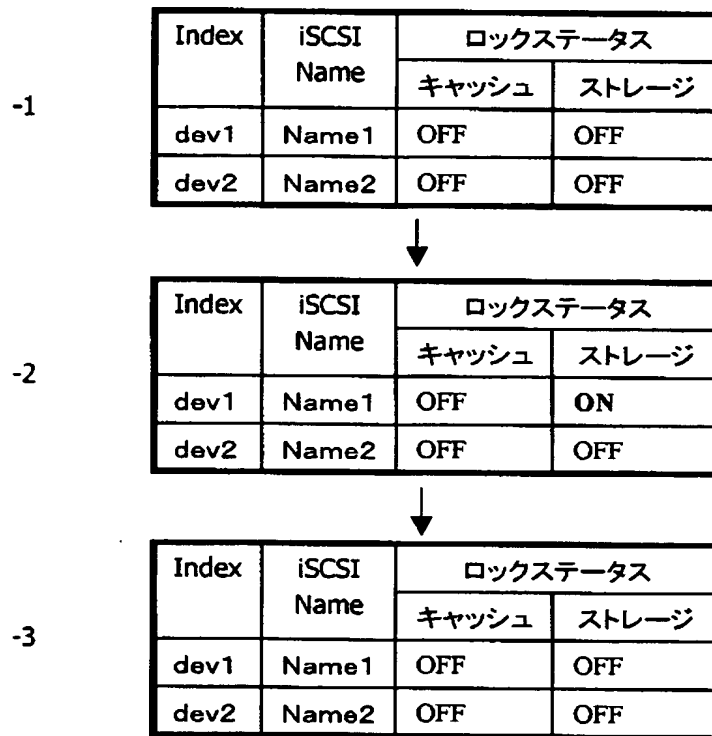
【図 7】

図7



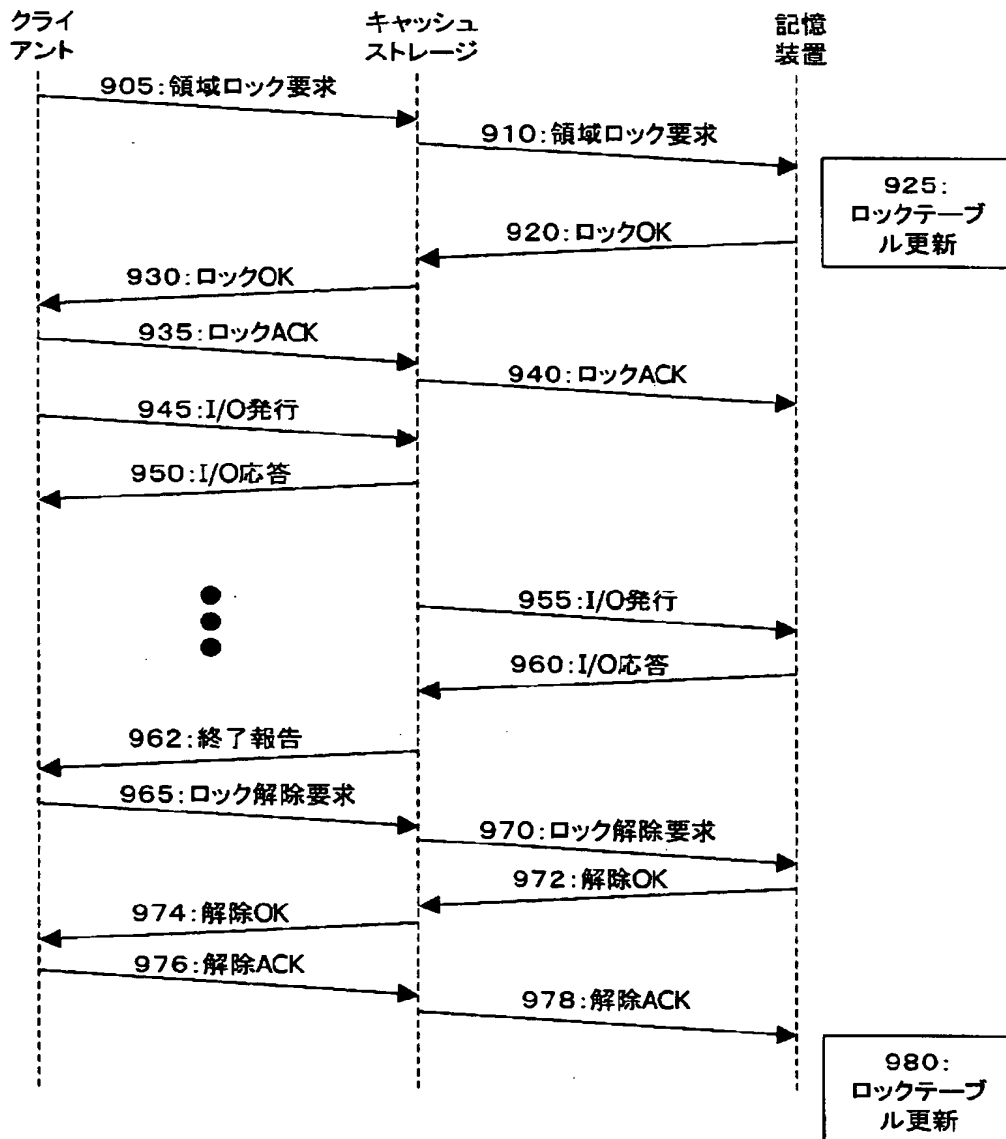
【図 8】

図8



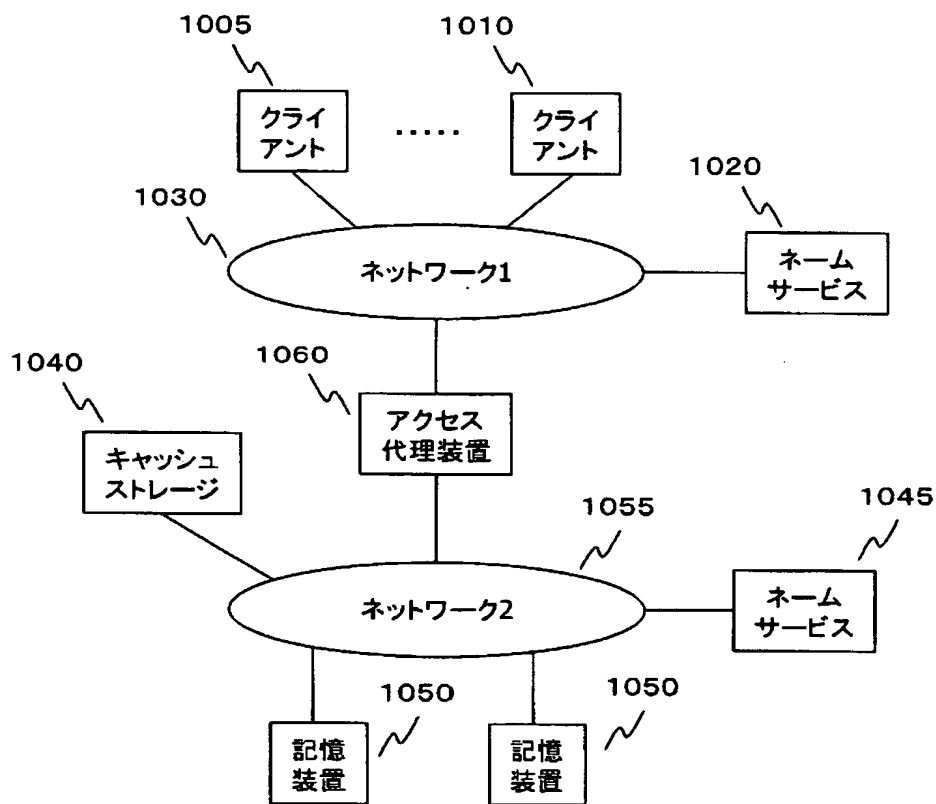
【図9】

図9



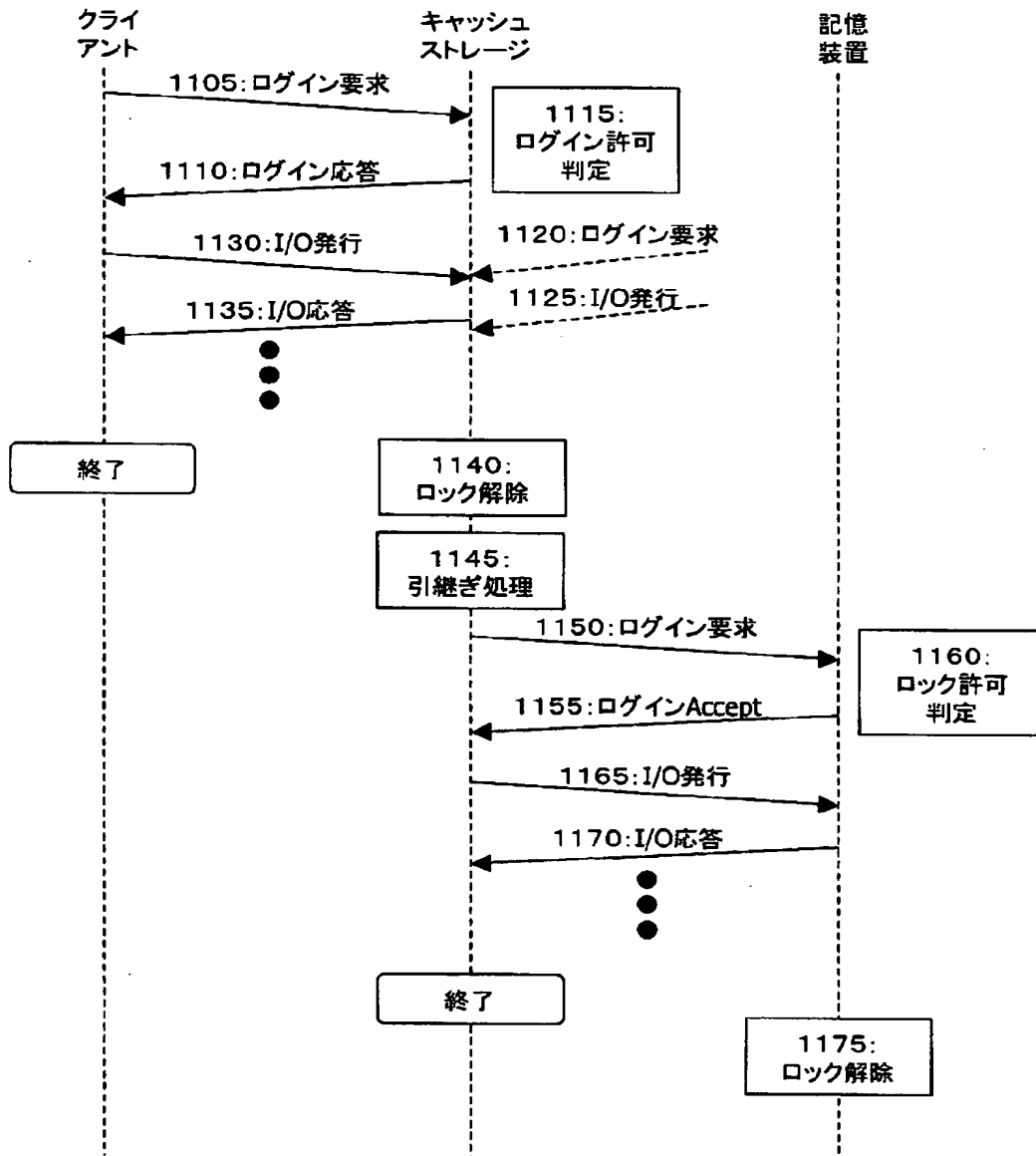
【図10】

図10



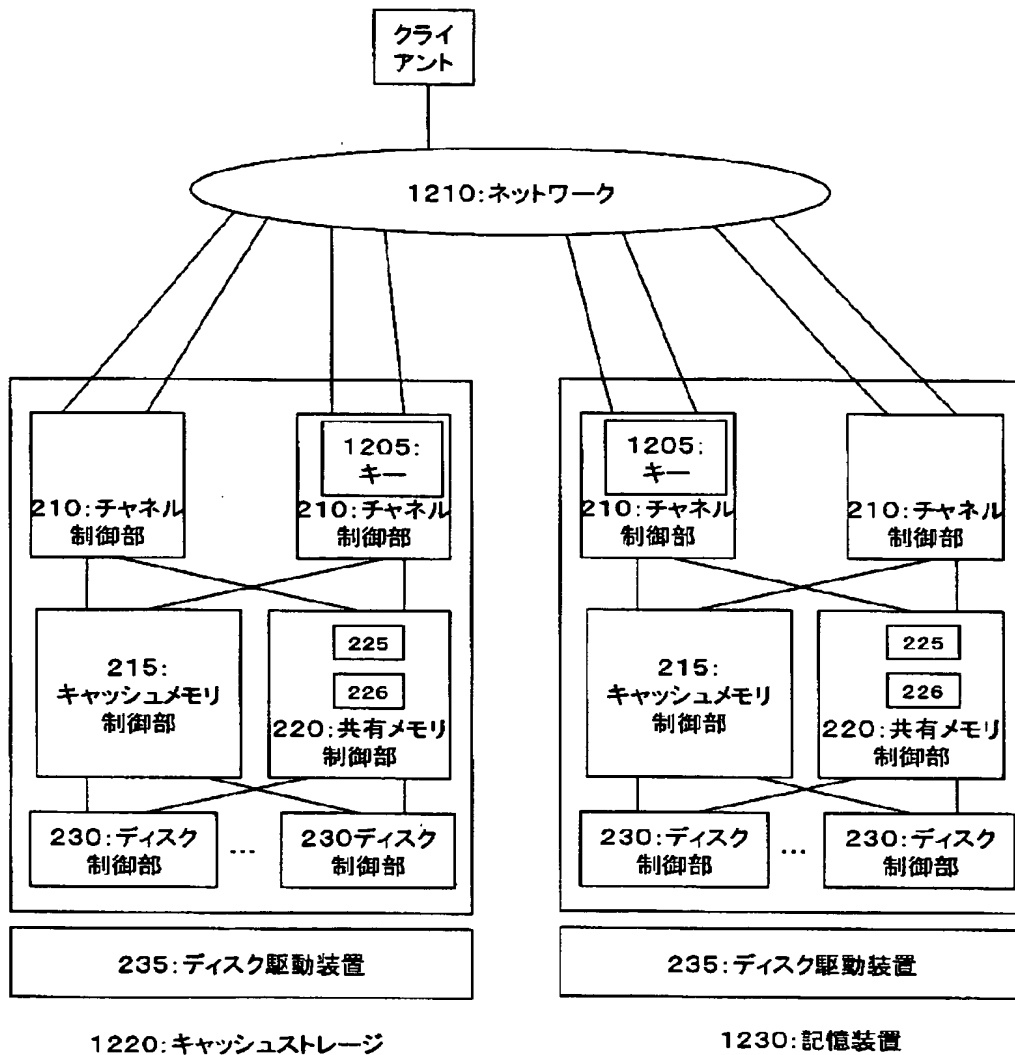
【図11】

図11



【図12】

図12



【図 13】

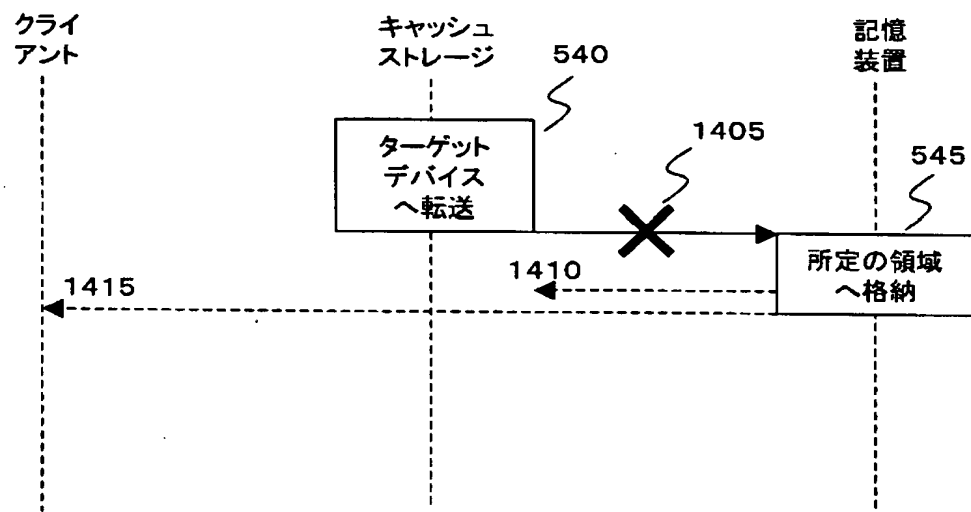
図13

1305: デバイス名	1310: アドレス
Dev1	Name1
Dev2	Name2
Dev3	Name3

1300

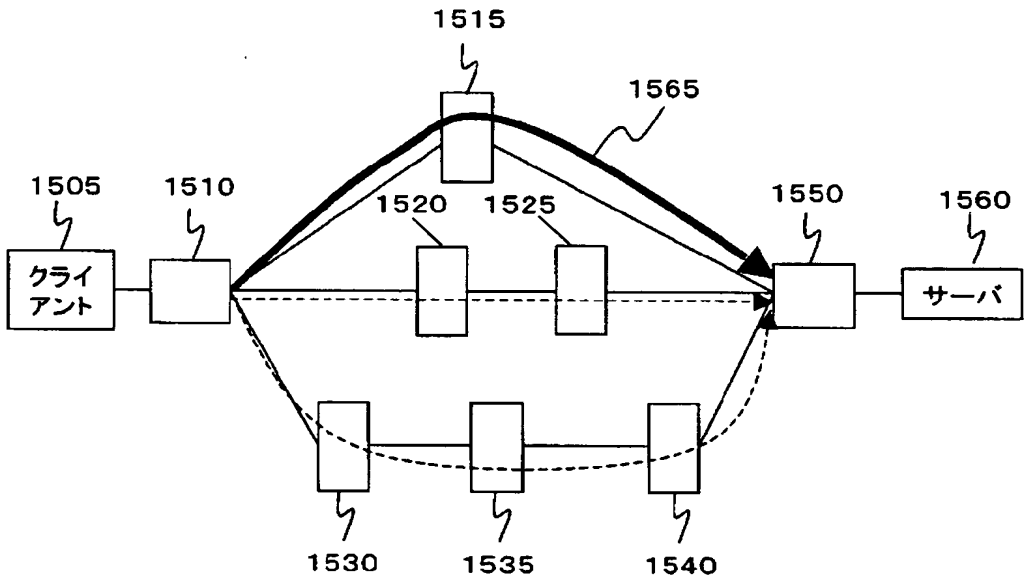
【図 14】

図14



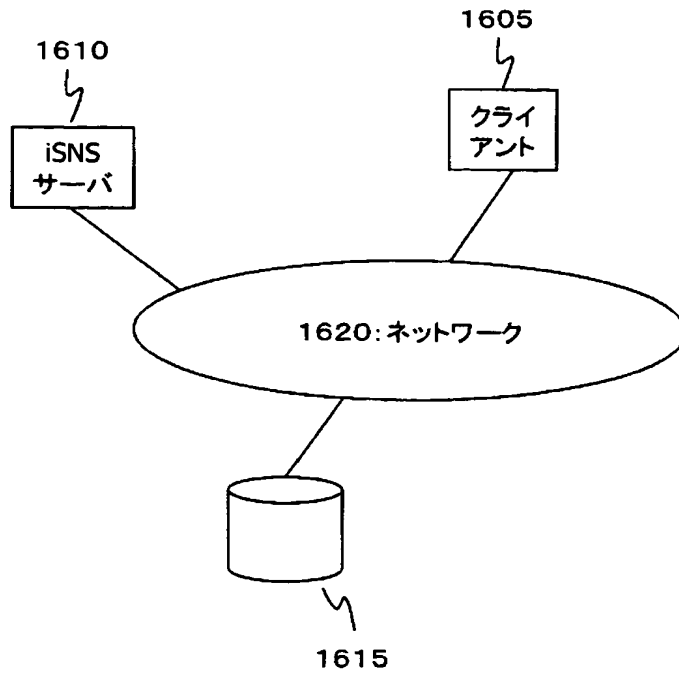
【図 15】

図15



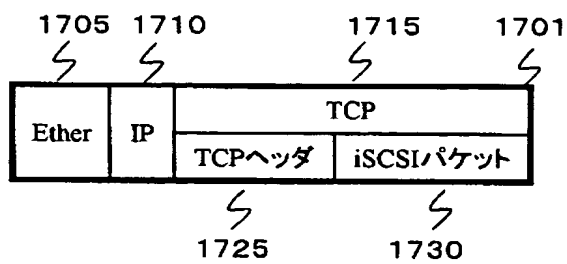
【図 16】

図16



【図 17】

図17



【書類名】 要約書

【要約】

【課題】 TCP/IPネットワークで通信する場合、伝送遅延、伝送路上の障害による再送処理で応答性能、トランザクション性能が劣化する。

【解決手段】 クライアントと記憶装置間にキャッシュストレージを設け、クライアントがアクセスする領域をあらかじめロック（排他）する。

【効果】 伝送遅延の軽減、再送処理時の通信距離の短縮によりクライアントから見た応答性能、トランザクション性能を改善出来る。

【選択図】 図1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 1 1 6 4 5 1
受付番号	5 0 3 0 0 6 6 0 6 4 9
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 4 月 2 3 日

< 認定情報・付加情報 >

【提出日】 平成15年 4月22日

次頁無

特願 2 0 0 3 - 1 1 6 4 5 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 1 0 8]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所